BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 11, Number 8 August 2011

The New UK Bribery Act And Data Protection Issues Involving Associated Persons, Including Suppliers And Employees

By Renzo Marchini, of Dechert LLP, London.

Introduction

The UK Bribery Act 2010 (the "Act") came into force on July 1, 2011, and brought with it both an extension and a simplification of the previous UK law on bribery and corruption (as well as the repeal of old offences) (*see analysis at WDPR, October 2010, page 4*).

There are four new criminal offences created by the Act. As well as the active offences of bribing (Section 1) and bribing a foreign public official (Section 6) and the passive offence of being bribed (Section 2), there is a strict liability offence of failing to prevent bribery (Section 7). It is this last offence which creates issues under data protection law.

The Act is accompanied by guidance[1] (the "Guidance") which was published on March 30, 2011, and assists with interpretation of an important defence (of having "adequate procedures") to this strict liability offence.

This article focuses on the tension which can arise between attempts to comply with the requirement to have adequate procedures to prevent bribery (which will often involve the collection and processing of personal data as part of the vetting or monitoring process) and attempts to remain compliant with data protection law.

The Strict Liability Offence

The strict liability offence of failing to prevent bribery is committed by a relevant commercial organisation if a person "associated with" that organisation bribes another person, with the intention of obtaining or retaining for the organisation any business or an advantage in the conduct of business.

The definition of an associated person is wide: An associated person is one who performs services for or on behalf of the organisation. This could include employees, agents, subsidiaries, contractors, suppliers or joint-venture partners. The associated person's nationality or the place where the bribe occurred is irrelevant.

The Act will apply to UK organisations or even foreign organisations which carry out business in the United Kingdom.

The Defence

The only defence to the strict liability offence is that the commercial organisation had "adequate procedures" in place. The Guidance sets out six principles which aim to assist organisations in preventing bribery. In considering these principles, the Guidance highlights that the aim is for organisations to achieve effective anti-bribery procedures whilst taking a proportionate and risk-based approach.

For present purposes, the two most important prin-

ciples are Due Diligence and Monitoring and Review. The former directs organisations to apply risk-based due diligence procedures in respect of persons associated with them and in respect of direct contractual counterparties. As part of this process, it is often likely that personal data will be collected. The latter requires that organisations monitor and review their anti-bribery procedures and make improvements where necessary.

Introduction to Data Protection Issues

Data protection rules in the United Kingdom are primarily set out in the Data Protection Act 1998 (the "DPA"); but from a point of substance (if not procedure and enforcement), the principles in the DPA relevant to the issues under discussion will be similar throughout the European Union, since they emanate from Directive 95/46/EC (the "Data Protection Directive", or "Directive"). The DPA and the Directive both apply to "personal data", which is data which relates to a living individual, the data subject, who can be identified from that data. It applies to data held electronically and to some data held in manual files.

The DPA makes a distinction between general personal data and "sensitive" personal data (in the Directive, the special categories of data). This is information of a particular type in relation to which the legislation gives a greater level of protection. Sensitive personal data will include information about an individual's commission or alleged commission of a criminal offence or related proceedings.

As is well-known, a data controller will have to ensure that it complies with the data protection principles (we continue using the terminology of the DPA, rather than that of the Directive). In particular, the person addressing Bribery Act compliance must ensure that the resulting personal data is "fairly and lawfully" processed and, in particular, that one of a limited number of conditions set out in the DPA is fulfilled, the most relevant of which will be discussed below.

Due Diligence on Suppliers

In order to make out a defence of "adequate procedures" to the strict liability offence of failing to prevent bribery, an organisation will want to carry out due diligence in relation to any organisation that might be associated with it, including suppliers.

Due diligence could entail a questionnaire being sent to a supplier for completion containing both general questions requesting information, such as bank details and a description of business undertaken, and more detailed questions relating to the supplier's constitutional documents, details of the supplier's subcontractors, shareholder or director details and details of any involvement with government officials. Due diligence may also involve searching in local trade registers, local criminal record databases (to the extent that data is available in any particular jurisdiction) and, in some circumstances, may even require enquiries by investigators. Inevitably, personal data will be collected, perhaps of the supplier itself (when an individual) or of shareholders or employees of the supplier.

Any such collection of data will have to satisfy at least one of certain conditions (set out in Schedule 2 of the DPA), the most relevant of which are:

1. The data subject has given his consent to the processing.

3. The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

6. The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

If the supplier is an individual, or an owner-managed small business where the owner is dealing with the enquiring organisation, then he is likely providing information only about himself, and consent should be fairly easily made out. However, if the supplier is a more substantial entity, then consent may be more difficult to achieve. The responding supplier may then be providing information about individuals in relation to whom it may not be practicable to obtain consent or who feel that they have no choice but to consent for fear of adverse employment consequences should they refuse (and any purported consent may then not be sufficient, as it may not be "freely given").

Another legitimising basis may need to be relied upon. The applicability of the third condition, regarding compliance with a legal obligation, is unlikely to be available for reasons discussed below.

We are left with one further contender, the sixth condition, regarding legitimate interests. A data controller can reason that the processing of data when performing due diligence on suppliers is necessary for the pursuit of a legitimate interest, namely being able to defend itself from a Bribery Act prosecution. However, there is a balance to be drawn against the prejudice that may arise in relation to the rights of the individuals concerned. Data protection law is well-versed in applying this test to different situations, and what is likely to be expected here is a proportionate application of diligence to the need to comply with the Bribery Act. In particular, a business should be wary of over-reaching by vetting supplier personnel at too low a level of responsibility, checks must be proportionate to the risk faced, and so on.

If the data that is processed is sensitive personal data (such as information regarding a person's alleged or actual criminal convictions), the data controller will also have to meet a more stringent condition (set out in the DPA in Schedule 3). The most relevant are set out below:

1. The data subject has given his explicit consent to the processing of the personal data.

6. The processing is necessary for the purpose of, or in connection with, any legal proceedings (including pro-

   ISSN 1473-3579

spective legal proceedings), is necessary for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Again, if the respondent is an individual answering questions about himself, then consent will likely be present. If this is not the case, the only remaining candidate Schedule 3 condition is that it may be arguable that the processing is necessary in connection with "establishing, exercising or defending legal rights", in that the processing is a necessary part of due diligence which may enable a business to defend itself (or pre-emptively establish a defence) against a bribery prosecution, as it could show it had adequate procedures in place. However, this is not clear-cut, and turns on whether complying with guidance and in other ways putting in place "adequate procedures" to prevent a crime is in fact the defence of "legal rights".

Due Diligence on Employees

Employees will also be considered persons who are associated with the business, and thus a business could be strictly liable in relation to its employees' activities, and will need to consider performing due diligence in order to show that adequate procedures were in place to prevent any wrongdoing. Similar data protection issues arise here as with the vetting of suppliers. In this context, however, businesses have the benefit of the UK Information Commissioner's Office's Employment Practices Code.

Although businesses may want to carry out extensive checks to ensure that any prospective employee will not be a liability in terms of Bribery Act prosecution, the Code makes clear, in a general vetting context (it was written before this Act was conceived), that checks must be proportionate and consideration should be given to the same types of factors as listed above in relation to suppliers.

If it is decided that the checks are proportionate and there is no alternative, the Code says that vetting should be carried out at as late a stage as possible in the recruitment process; vetting should be used to obtain only specific information; and information should be sought only from likely sources of relevant information, and, if it is necessary to obtain information from third parties, signed consent should be obtained from the job applicant.

There are certain industries, for example, the financial services industry, where employers may wish to undertake criminal records checks on prospective employees. The sort of data revealed by such checks will be sensitive personal data, and so the Schedule 3 conditions discussed above should be complied with along with the Code guidance. Given the direct relationship between the individual applicant for a position and the vetting organisation, there will be explicit consent. Indeed, the Code of Practice in relation to Criminal Records Bureau (CRB) checks[2] (when the individual is employed in the United Kingdom) must also be complied with — and that also requires a form to be signed by the individual which gives the consent necessary. If a search is made in a foreign country which does not require consent (under its rules for searching criminal records), that fact would not absolve the organisation from complying with the DPA requirement to obtain consent.

Whistleblowing

The coming into force of the Act is likely to result in more businesses setting up hotlines to demonstrate that they have adequate procedures in place to prevent bribery. These hotlines will need to comply with data protection legislation. This raises similar issues to the conflict that exists between whistleblowing hotlines that are required under the U.S. Sarbanes-Oxley Act of 2002 ("SOX") for publicly held U.S. companies and their EU-based affiliates, and EU data protection legislation.

The processing of personal data arising from the operation of that hotline again has to satisfy a relevant Schedule 2 or Schedule 3 condition. The most relevant conditions in this case are that the processing must be necessary for compliance with a legal obligation, or for the purpose of a legitimate interest pursued by the company to which the data is disclosed. It is likely that assisting in demonstrating adequate procedures could similarly be deemed a legitimate interest.

In addition, there are other important data protection principles to be considered. The third data protection principle is that personal data must not be excessive in relation to the purpose for which it is held, and the fifth principle is that personal data must not be kept for longer than is necessary for the processing purpose. These principles highlight the conflict between Bribery Act compliance considerations (encouraging businesses to find out as much as they can about suppliers and employees to underpin a possible need to show "adequate procedures") and the underlying tenet of data protection legislation that requires businesses to minimise data.

The recommendations of the EU Article 29 Data Protection Working Party in relation to SOX might be considered useful in the Bribery Act context as unofficial guidance on how any anti-bribery hotlines should be operated. These recommend such steps as minimising the number of people who can use the hotlines (or who can be reported through them); anonymous reports should not be encouraged and, in particular, should not be advertised; data collected should be kept to a minimum and retained for as short a time as possible (usually to be deleted within two months); being transparent as to the destination of the reports and as to the fact of confidentiality of the whistleblower; and using internal resources (rather than outsourced service providers) if possible. Moreover, anyone accused should be informed of a report (unless it would jeopardise the company's ability to investigate).

Conclusion

The Bribery Act has received much attention in relation to the steps that businesses will need to take to ensure

their compliance with the new rules. Much less has been said of the data protection aspects.

When making plans for Bribery Act compliance, businesses will need to assess carefully the new procedures and policies they are implementing and what that means from a data protection standpoint, as there will inevitably be conflicts between obtaining as much information as possible about employees and suppliers to avoid Bribery Act risk and minimising the processing of information to comply with data protection obligations. In undertaking sensitive checks, consideration ought to be given to obtaining consent from all relevant employees.

NOTES

[1] "The Bribery Act 2010: Guidance about procedures which relevant commercial organisations can put into place to prevent persons associated with them from bribing", available at http://www.justice.gov.uk/downloads/guidance/making-reviewing-law/bribery-act-2010-guidance.pdf

[2] Note that the UK CRB check regime has recently been reviewed with changes being made (see Protection of Freedoms Bill), such as CRB certificates being issued only to an applicant so that disputed information is not seen by the employer. There is a second phase of review being undertaken which will consider how criminal records should be defined, managed, used and stored, and a report is awaited.

Renzo Marchini is Counsel in the London office of Dechert LLP and a member of the World Data Protection Report Editorial Board. He may be contacted at renzo.marchini@dechert.com.

  WDPR ISSN 1473-3579